A cryptographic method to send a secret route or map to a receiver using concepts in graph theory and number theory

S.A.S. Sureni Wickramasooriya, Thisal M. Weerasekara, G.H. Jayantha Lanel, T.P. de Silva, N.C. Ganegoda

Abstract— **Even though new solutions for problematic situations arising from security norms are developing day by day, possibly there are some issues remaining on our hand yet to be tackled. Among those one of the major problem for almost every country might experience is routing and mapping secrecy. In detail, when sending someone's route of some places or sending a map of protectorate places, its secrecy is the most important factor to be considered. In this study a system is developed which could be used to send a route of a particular person or a map of some specific secret place in a secret manner. Concepts in graph theory and number theory together with some cryptographic algorithms are used to develop this system. In brief, the route or map is transformed into a graph which might be directed or non-directed. Then it simplified in to a numerical value which could be encrypted by applying particular encrypting algorithm. Thereafter, encrypted numerical code is sent to the receiver. Once receiver receives that unreadable code then he/she applies decrypting algorithm on that to obtain the original numerical value. Finally, the graph can be derived from that numerical value and it could be regarded as the map or route that has been sent. However different methods are followed to send the map or route due to the directivity of the graph. Although there are some restrictions and assumptions which have been made during the process, there may be possibilities to further improve this system.**

Index Terms— **Cipher text, Decryption, Directed graph, Encryption, Non-directed graph**.

I. INTRODUCTION

Cryptography has played an enormous role in the shaping and development of many societies and cultures. Cryptography probably began in or around 2000 B.C. in Egypt, where hieroglyphics were used to decorate tombs of deceased rulers and kings which represents the story of the life of the king and proclaimed the great acts of his life. Cryptography is the science that has been used for many years to translate messages into secret format and getting the real message from the secret format. Though cryptography has begun with very small techniques such as symbols, with the rise of the information age, computers have bought it to a whole new level. In 1553, Giovan Batista Belaso came up with idea of the password. In world war II, mechanical and electromechanical cipher machines were widely used.

S.A.S. Sureni Wickramasooriya, Department of Mathematcs, Faculty of Engineering, University of Moratuwa, Sri Lanka, +94716961356.
Thisal M. Weerasekara, Department of Mathematcs, Faculty of Applied Sciences, University of Sri Jayewardenepura, Sri Lanka, +94714480113**G.H. Jayantha Lanel**, Department of Mathematcs, Faculty of Applied Sciences, University of Sri Jayewardenepura, Sri Lanka, +94112758384
T.P. de Silva, Department of Mathematcs, Faculty of Applied Sciences, University of Sri Jayewardenepura, Sri Lanka, +94112758377
N.C. Ganegoda, Department of Mathematcs, Faculty of Applied Sciences, University of Sri Jayewardenepura, Sri Lanka, +94112758380

In some situations, one's route should be very critical and secret. As an example, when the leader of a country is in an official visit to the part of his own country or to another country, that visit should be very secret. If his route is disclosed by enemy there may arise many security and confidential problems. Therefore this emphasizes the necessity of possessing a route in a secret way for an imperative person.

The protection of routes in a plan of protector places such as military camps is very essential. Therefore the other application is based on sending a secret map to a recipient in a secure manner. If there is no any proper method of sending the map in a secret way there will be malignant attacks. The combination of cryptographic algorithms and graph theoretical concepts can be used to solve these problematic situations up to some extent. In brief, the objective of this research is to convert a graph or map into an encrypted numerical value which can be easily sent to a receiver without any hesitation. Furthermore this contains the process of building up the secret map or route by the receiver. More importantly software with MATLAB which could implement this procedure by generating the numerical value from the graph and decrypting it to generate the graph back is developed to give more reliable solution.

II. METHODOLOGY

The first step is converting the map or route in to a graph. Here the roads are represented by edges and junctions or cities or countries can be represented by vertices. Map is represented by a non-directed graph while the route is represented by a directed graph. Then the constructed graph is transformed into adjacency matrix. A new procedure is followed to calculate the numerical value from the adjacency matrix. Calculation part varies according to the directivity (a map or route) of the graph.

Sending a secret map and reconstructing back

Let takes the adjacency matrix of the graph as, $A = \{a_{ij}\}$ where $a_{ij} \in \{0,1\}$ with $a_{ii} = 0$ for $i, j = 1,2, \dots, n$

In this approach, the graph related to map is symmetric. Due to the symmetric attribute of non-directed graph, the upper triangular matrix is equal to the transpose of lower triangular matrix.
Generally, the adjacency matrix can be represented as follows.

$$A = \begin{pmatrix} 0 & a_{12} & \dots\dots\dots & a_{1n} \\ a_{12} & 0 & \dots\dots\dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ a_{1(n-1)} & a_{2(n-1)} & \vdots & a_{(n-1)2} \\ a_{1n} & a_{2n} & \vdots & 0 \end{pmatrix}$$

One triangle is enough to recognize the adjacency matrix however the sender and receiver must agree upon on the value that is to represent the upper triangular matrix or lower triangular matrix. In this study, 1 is referred to represent upper triangular matrix and 2 for lower triangular matrix.

Calculating the numerical value for non-directed graph

At first, all the binary digits of upper triangular matrix is written as one number with starting from the last row and for each row the direction should be right to left. Then this binary number connected to a decimal number d,

$$d = a_{12} \times 2^{x} + a_{13} \times 2^{x-1} + \ldots + a_{(n-2)n} \times 2^{1} + a_{(n-1)n}$$

$$\text{where } x = \frac{n^2-n}{2} \qquad (1)$$

Since the upper triangular matrix involves in calculation, 1 is affixed to the last digit of the decimal addition d, which is considered as the single numerical value ($d1$) and then it is encrypted by Rivest-Shamir-Adleman (RSA) algorithm to get the secret code(α). This code is sent to the receiver who can derive the real map or route after applying some reverse process.

Reconstructing the map

After receiving the cipher text, then it is the deciphered to get the numerical value. Since the last digit of the numerical value represents upper triangular or lower triangular attribute. The numerical value except the last digit is considered to develop the relevant adjacency matrix. It is converted into a binary number. If the last digit of plaintext is 1, then the upper triangular matrix is constructed from the binary number calculated. The order of filling is row-wise. Here the first right most digits represent the last entry of the top row to last row. By continuing this process the upper triangular matrix is derived. The lower triangular matrix is constructed by getting the transpose of the upper triangular matrix and the adjacency matrix is produced by putting them together.

Sending a secret route and reconstructing back

In here a route will produce a directed graph as a result of that adjacency matrix of the graph is not symmetric. Therefore we have to send two secret codes for upper and lower triangular matrices.

Let the matrix as follows,

$$A = \{a_{ij}\} = \begin{pmatrix} 0 & a_{12} & \ldots\ldots\ldots & a_{1n} \\ a_{21} & 0 & \ldots\ldots\ldots & a_{2n} \\ : & : & : & : \\ : & : & : & : \\ a_{(n-1)1} & a_{(n-1)2} & : & a_{(n-1)n} \\ a_{n1} & a_{n2} & : & 0 \end{pmatrix}$$

where $a_{ij} \in \{0,1\}$.

Numerical value consisting last digit 1 will represent the upper triangular matrix and on the other hand numerical value with last digit 2 will be the numerical value representing the lower triangular matrix. The addition of upper and lower triangular matrices is the adjacency matrix related to that particular directed graph.

Calculating the numerical value for directed graph.

Turning in to the directed graph, a method followed to derive the numerical code of upper triangular matrix is similar to the method followed in non-directed graph in previous section.

For upper triangular matrix

$$A = \begin{pmatrix} 0 & a_{12} & \ldots\ldots\ldots & a_{1n} \\ & 0 & \ldots\ldots\ldots & a_{2n} \\ : & : & : & : \\ : & : & : & : \\ & & : & a_{(n-1)n} \\ & & : & 0 \end{pmatrix}$$

$$d_1 = a_{12} \times 2^{x} + a_{13} \times 2^{x-1} + \ldots + a_{(n-2)n} \times 2^{1} + a_{(n-1)n}$$

where $x = \frac{n^2-n}{2}$

After applying encrypting algorithm to $d_1 1$ the secret code (α_1) of upper triangular matrix can be derived.

For lower triangular matrix

$$A = \begin{pmatrix} 0 & & \ldots\ldots\ldots & \\ a_{21} & 0 & \ldots\ldots\ldots & \\ : & : & : & : \\ : & : & : & : \\ a_{(n-1)1} & a_{(n-1)2} & : & \\ a_{n1} & a_{n2} & : & 0 \end{pmatrix}$$

$$d_2 = a_{21} \times 2^{x} + a_{31} \times 2^{x-1} + \ldots + a_{n(n-2)} \times 2^{1} + a_{n(n-1)}$$

where $x = \frac{n^2-n}{2}$

After applying encrypting algorithm to $d_2 2$ the secret code (α_2) of upper triangular matrix can be derived.

Once the receiver receives the cipher text, they would decipher it to reconstruct the graph as follows.

Reconstructing the route

In this category the receiver receives two cipher texts α_1 and α_2.

The first step is decrypting two cipher texts to disclose the original numerical values $d_1 1$ from α_1 and $d_2 2$ from α_2. After that, the last digits of $d_1 1$ and $d_2 2$ should be removed to disclose d_1 and d_2 which can be used to derive upper and lower triangular matrices. The addition of those two matrices will produce the relevant adjacency matrix.

Thus the adjacency matrix of graph would be used to develop the particular route.

Construction of Adjacency matrix of a Non-directed graph

Input : Number of vertices of the graph(n),

Output : Adjacency matrix of the graph (A)

1) $i \coloneqq 1$
1.1) $j \coloneqq 1$
1.1.1) $\boldsymbol{If}\ i\ and\ j\ connected, \boldsymbol{then}\ \ A(i,j) \coloneqq 1,$
$\boldsymbol{Otherwise}, A(i,j) = 0$
1.1.2) $j \coloneqq j + 1$
1.1.3) $\boldsymbol{If}\ j < n, go\ to\ step\ (1.1.1),$
$\boldsymbol{Otherwise}\ go\ to\ step\ (1.2)$
1.2) $i \coloneqq i + 1$
1.3) $\boldsymbol{If}\ i < n, \boldsymbol{then}\ go\ to\ step\ 1.1),$
$\boldsymbol{Otherwise}\ output$
$adjacency\ matrix\ (A)$

Encryption of the Non-directed Graph

Function Non_Directed_Graph (A) {return $\boldsymbol{d}$}

Input : Adjacency matrix (A)
Output : Numerical value (nm)

1) $N \coloneqq Number\ of\ rows\ in\ A$
2) $i \coloneqq 1$
2.1) $j \coloneqq 1$
2.1.1) $A(i,j) \coloneqq 0$
2.1.2) $j \coloneqq j + 1$
2.1.3) $If\ j < i, then\ go\ to\ step\ (2.1.1),$
$Otherwise\ go\ to\ step\ (2.2)$
2.2) $i \coloneqq i + 1$
2.3) $If\ i < N, then\ go\ to\ step\ (1.1),$
$Otherwise\ return\ A$
3) $n \coloneqq (N-1)\ th\ triangular\ number$
4) $\boldsymbol{d} \coloneqq 0$
5) $i \coloneqq 1$
5.1) $j \coloneqq i + 1$
5.1.1) $\boldsymbol{d} \coloneqq \boldsymbol{d} + A(i,j) \times 2^n$
5.1.2) $j \coloneqq j + 1$
5.1.3) $If\ j < N, go\ to\ step\ (5.1.1),$
$Otherwise\ go\ to\ step\ (5.2)$
5.2) $i \coloneqq i + 1$
5.3) $If\ i < N - 1, go\ to\ step\ (4.1),$
$Otherwise\ return\ \boldsymbol{nm}$
6) $\boldsymbol{d1} \coloneqq \boldsymbol{d} \times 10 + 1$

Decryption of the Non-directed Graph

Function Undirected _graph_inv ($\boldsymbol{d1}$) {return A }

Inputs : numerical value (nm)
Output: Adjacency matrix (A)

% Removing the least significant digit which indicate that is a UTM

1) $\boldsymbol{d} \coloneqq (\boldsymbol{d1} - 1)/10$
2) $\boldsymbol{d} \coloneqq binary\ value\ of\ the$
$decimal, \boldsymbol{d}$

% Construction of the required UTM

3) $N \coloneqq length\ of\ \boldsymbol{d}$
$(number\ of\ digits\ in\ \boldsymbol{d})$

*% Determine kth triangular number, **N***

4) $k \coloneqq 0$
5) $s \coloneqq 0$

6) $Check\ whether\ s \neq N,$
$If\ so\ go\ to\ step\ (6.1),$
$Otherwise\ go\ to\ step\ (7)$
6.1) $k \coloneqq k + 1$
6.2) $s \coloneqq s + 1$
6.3) go to step 6)
7) $i \coloneqq 1$
7.1.1) $j \coloneqq 1$
7.1.2) $U(i,j) \coloneqq \boldsymbol{d}(r)$
7.1.3) $j \coloneqq j + 1$
7.1.4) $If\ j < k + 1, then\ go\ to\ step\ (7.1.1),$
$Otherwise\ go\ to\ step\ (7.2)$
7.2) $i \coloneqq i + 1$
7.3) $If\ i < k, then\ go\ to\ step\ 7.1,$
$Otherwise\ go\ to\ step\ 8$
7) $Add\ a\ row\ with\ zero\ elements$
$to\ matrix\ U$
% Construction of required $\boldsymbol{LTM}$
9) $i \coloneqq k + 1$
9.1) $j \coloneqq 1$
9.1.1) $L(i,j) \coloneqq U(j,i)$
9.1.2) $j \coloneqq j + 1$
9.1.3) $If\ j < k + 1, then\ go\ to\ step\ (9.1.1),$
$Otherwise\ go\ to\ step\ (9.2)$
9.2) $i \coloneqq i + 1$
9.3) $If\ i < k + 1, then\ go\ to\ step\ (9.1),$
$Otherwise\ go\ to\ step\ (10)$
10) $A \coloneqq U + L$

Construction of Adjacency matrix of a directed graph

Input : Number of vertices of the graph(n)

Output : Adjacency matrix of the graph (A)

1) $i \coloneqq 1$
1.1) $j \coloneqq 1$
1.1.1) $if\ i\ and\ j\ connected\ and$
$the\ direction\ is\ i \rightarrow j\ then,$
$A(i,j) \coloneqq 1$
$Otherwise, A(i,j) \coloneqq 0$
1.1.2) $j \coloneqq j + 1$
1.1.3) $if\ j < n, go\ to\ step\ (1.1.1),$
$Otherwise\ go\ to\ step(\ 1.2)$
1.2) $i \coloneqq i + 1$
1.3) $If\ i < n, go\ to\ step\ (1.1),$
$Otherwise\ output$
$adjacency\ matrix\ (A)$

Encryption of the Directed Graph

Function Directed_Graph (A) { return $\boldsymbol{d1}$, $\boldsymbol{d2}$ }

Input : Adjacency matrix (A)
Output : Numerical values $\boldsymbol{a}$ and $\boldsymbol{b}$

1) $N \coloneqq Number\ of\ rows\ in\ A$

2) $k \coloneqq 0$
3) $i \coloneqq 1$
3.1) $k \coloneqq k + i$
3.2) $i \coloneqq i + 1$
3.3) $If\ i < N - 1, then\ go\ to\ step(3.1),$
$Otherwise\ go\ to\ step(4)$
4) $n \coloneqq k - 1$ % the triangular number

% Calculating numerical ***value a***

5) $\boldsymbol{d2} \coloneqq 0$

6) $i \coloneqq 2$
6.1) $j \coloneqq 1$
6.1.1) $\boldsymbol{d2} \coloneqq \boldsymbol{d2} + M(i,j) \times 2^n$
6.1.2) $n \coloneqq n - 1$
6.1.3) $j \coloneqq j + 1$
6.1.4) $If\ j < i - 1, then\ go\ to\ step$ 6.1.1),
$Otherwise\ go\ to\ step$ (6.2)
6.2) $i \coloneqq i + 1$
6.3) $If\ i < N\ then, go\ to\ step$ (6.1),
$Otherwise\ go\ to\ step$ (7)
7) $\boldsymbol{d_2 2} \coloneqq \boldsymbol{d2} * 10 + 2$
% Calculation of numerical ***value b***
8) $\boldsymbol{d_1 1} = return\ value\ of\ function$
$Non\_Directed\_Graph(A)$

Decryption of the Directed Graph

Function Directed_graph_inv($\boldsymbol{d_1 1}$, $\boldsymbol{d_2 2}$) {return A }

Inputs : Numerical values $\boldsymbol{a}$ and $\boldsymbol{b}$
Outputs : Adjacency Matrix (A)

% Reconstruction of $\boldsymbol{d1}$ *and* $\boldsymbol{d2}$

1) $\boldsymbol{d2} \coloneqq (\boldsymbol{d_2 2} - 2)/10$
% $\boldsymbol{d2}$ represents the LTM

2) $\boldsymbol{d1} \coloneqq (\boldsymbol{d_1 1} - 1)/10$
% $\boldsymbol{d1}$ represents the UTM
3) $N \coloneqq Number\ of\ elements\ in$
$array\ \boldsymbol{d1}$
% Calculation of the triangular number
4) $k \coloneqq 0$
5) s $\coloneqq 0$
6) $when\ s\ not\ equals\ N, go\ to\ step$ (6.1),
$Otherwise\ go\ to\ step$ (7)
6.1) $k \coloneqq k + 1$
6.2) $s \coloneqq s + k$
6.3) $go\ to\ step$ (6)
% Converting $\boldsymbol{d2}$ *and* $\boldsymbol{d1}$ *to binary*
7) $\boldsymbol{bina} \coloneqq binary\ value\ of$
$decimal, \boldsymbol{d2}$
9) $\boldsymbol{binb} \coloneqq binary\ value\ of$
$decimal, \boldsymbol{d1}$
% Construction of Corresponding ***UTM***
9) $r \coloneqq 0$
10) $i \coloneqq 1$
10.1) $j \coloneqq i + 1$
10.1.1) $r \coloneqq r + 1$
10.1.2) $U(i,j) \coloneqq value\ of\ \boldsymbol{binb}\ in$
$the\ index\ of\ r$
10.1.3) $j \coloneqq j + 1$
10.1.4) $If\ j < k + 1, go\ to\ step$ (10.1.1),
$Otherwise\ go\ to\ step$ (10.2)
10.2) $i \coloneqq i + 1$
10.3) $If\ i < k,\ then\ go\ to\ step$ (10.1),
$Otherwise\ go\ to\ step$ (11)
% Construction of Corresponding ***LTM***
11) $l \coloneqq 0$
12) $i \coloneqq 2$
12.1) $j \coloneqq 1$
12.1.1) $l \coloneqq l + 1$
12.1.2) $L(i.j) \coloneqq value\ of\ \boldsymbol{bina}\ in$
$the\ index\ of\ l$
12.1.3) $j \coloneqq j + 1$
12.1.4) $If\ j < i - 1, go\ to\ step$ (12.1.1),

$Otherwise\ go\ to\ step$(12.2)
12.2) $i \coloneqq i + 1$
12.3) $If\ i < k + 1\ then\ go\ to\ step$ (12.1),
$Otherwise\ go\ to\ step$ (13)
13) $Adjacency\ Matrix,\ A \coloneqq U + L$

III. RESULTS AND EVALUATIONS

Under this section some real world examples are provided to support the procedure developed in methodology.

Real world Mapping problem

This problem is mainly related with a map of a protective area. Let's consider the map given in Figure 1 is to be secretly sent to a trusted party. First the sending party and receiver must be agreed upon to an algorithm which is used for encrypting and decrypting. The sending party summarizes the map into a graph. Since this is a map the graph to be chosen is non-directed. Thus vertices can be selected as junction points which are the intersecting points of roads. Moreover roads connecting cities are considered to be edges of the graph.

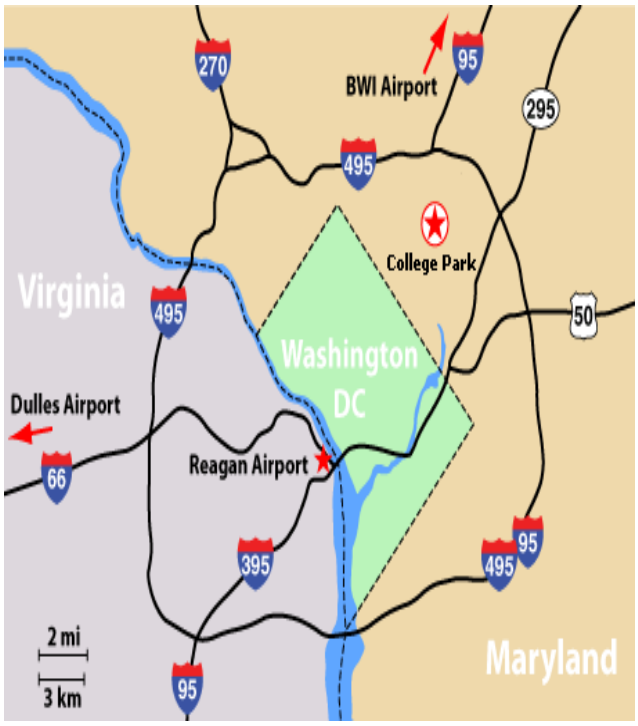

Figure 1

First the map should be summarized into a graph. The related graph of the map is represented in Figure 2.

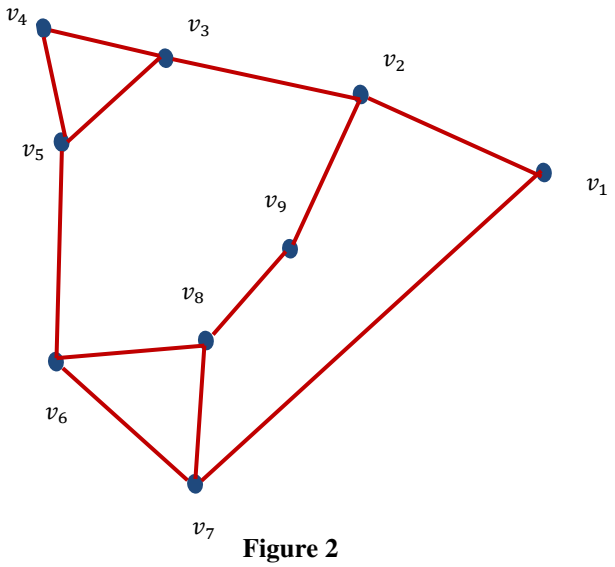

Figure 2

The adjacency matrix for the graph in Figure 2 is given by,

$$A = \begin{bmatrix} 0&1&0&0&0&0&1&0&0 \\ 1&0&1&0&0&0&0&0&1 \\ 0&1&0&1&1&0&0&0&0 \\ 0&0&1&0&1&0&0&0&0 \\ 0&0&1&1&0&1&0&0&0 \\ 0&0&0&0&1&0&1&1&0 \\ 1&0&0&0&0&1&0&1&0 \\ 0&0&0&0&0&1&1&0&1 \\ 0&1&0&0&0&0&0&1&0 \end{bmatrix}$$

Consider the following upper triangular matrix of the adjacency square matrix with size 9.

$$U = \begin{bmatrix} 0&1&0&0&0&0&1&0&0 \\ 0&0&1&0&0&0&0&0&1 \\ 0&0&0&1&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&1&1&0 \\ 0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&0&0&0 \end{bmatrix}$$

By(1), $\boldsymbol{d = 1 \times 2^{36} + 0 \times 2^{35} + \cdots + 0 \times 2^{1} + 1 \times 2^{0}}$

$\boldsymbol{= 355713848850}$

To represent the upper triangular matrix, 1 is written at the end of d. As a result the numerical value to be sent is, $d1 = 355713848851$

Then $d1$ is converted in to a secret code with the enciphering function of RSA and thereafter it will be sent to the receiver.

Implementation of Encrypting and Decrypting using RSA Algorithm

Input value $d1 = 355713848851$

1. Choose two primes p=5 and q=7
2. Compute $n = 5 \times 7 = 35$
3. Compute $\emptyset(n) = (p-1) \times (q-1)$
   $= 4 \times 6 = 24$
4. Choose e such that $1 < e < \emptyset(n)$
   and gcd $(e, n) = 1$; $e = 11$
5. Compute d such that
   $(d \times e) mod\ \emptyset(n) = 1$; $(d \times 11) mod\ 24 = 1$ then $d = 11$
6. Public key $= (e, n) = (11,35)$
   Private key $= (d, n) = (11,35)$
7. Encrypt with public key
   $\alpha = (d1)^e mod\ (n)$
   $= (355713848851)^{11} mod\ (35)$

Secret code of the matrix

α =12, 10, 10, 28, 1, 12, 22, 9, 22,10,1

8. Decrypt with private key
   $d1 = (\alpha)^d mod\ (n)$
   $= (\alpha)^{11} mod\ (35)$

After receiving the secret code(α), first it is decrypted and ignored the last digit to get the numerical value$(\ d)$. Then it is translated into the binary number and by using reverse process as explained in the methodology the adjacency matrix related to the graph could be derived. The graph represents the map of that considered protectorate area.

A real world routing problem

This problem is basically based on the official visit of the President of United States of America. His route lies through seven main cities in USA. The safe officers want to inform his route to other trusted parties secretly. The problem is the trusted and secret way to deliver the route. The developed concepts described in methodology can be used to solve this problem.

The President will be starting his visit from Washington and follow his trip as in the map.

Figure 3

The vertices of his route can be labelled as follows:

Washington-v_1, Chicago-v_2, Denver-v_3, Santa Fe-v_4, Poland-v_5, Los Angeles-v_6 and Miami-v_7.

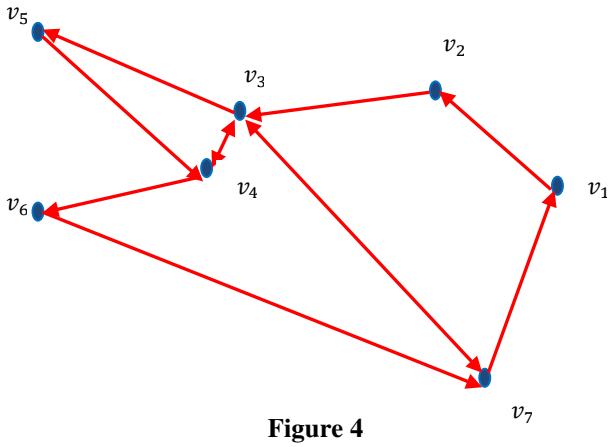

Figure 4

Moreover his route is given by

$$\{v_1\ v_2\ v_3\ v_4\ v_3\ v_7\ \ v_3\ v_5\ v_4 v_6\ v_7\ v_1\}$$

The adjacency matrix of the graph is,

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Since this is an adjacency matrix of directed graph, by following the steps in methodology (calculations the numerical value of directed graph) two numerical values $d_1 1$ and $d_2 2$can be obtained.

$$U = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad L = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$d_1 = 10658090 \longrightarrow d_1 1 = 10658091$

$d_2 = 34856 \longrightarrow d_2 2 = 348562$

After that numerical values are separately converted into the cipher text α_1 and α_2 which could be sent to the trusted parties

Here the enciphering function of RSA algorithm can be used to derive the secret codes α_1 and α_2.

$\alpha_1 = 1, 0,6,10,22,0,4,1$ and $\alpha_2 = 12,9,22,10,6,18$

When the receiver accepts these cipher texts they first decipher with the deciphering function of the considered algorithm to obtain the values d_1 from α_1 and d_2 from α_2 . The reverse process explain in methodology could be applied to construct the graph. The graph will illustrate the route of the President.

IV. DISCUSSION AND CONCLUSION

The two procedures followed for summarizing graphs into a secret value differ according to the directivity of the graph. In directed graph, representing upper triangular matrix by 1 and lower triangular matrix by 2 might be useful as a security tool. RSA algorithm is used in enciphering and deciphering tasks.

Even though there are some assumptions and restrictions in the procedure development, this method can be used to find real world solution for problematic situations arising in sending a map or route in a secure way. Furthermore this can be further developed with adding more theoretical concepts in graph theory and cryptography.

REFERENCES

[1] Boneh, D. (1998 , November). *Twenty Years Attacks on the RSA Algorithm.* Retrieved Auguest 24, 2013, from http://crypto.stanford.edu/~dabo/abstracts/RSAattack-survey.html

[2] Di, P. K. (2008, May 16). *Cryptozine*. Retrieved Aguest 25, 2013, from http://cryptozine.blogspot.com/2008/05/brief-history-of-cryptography.html

[3] Hahn, B. D. (2002). *Essential Mathlab for Scientist and Engineers.* Cape Town: Creda Communication.

[4] Harary and Frank. (1969). *Graph Theory.* Philippines: Addition-Wesley publishing company.

[5] Jonathan L. Gross , Jay Yellen. (2011). *Graph Theory and Its Application.* Boca Raton: Chapman and Hall/CRC.

[6] Jonathan L. Gross and Jey Yellen. (2004). *Hand Book of Grpah Theory.* Florida: CRC Press.

[7] Narsingh, D. (2008). *Graph theory with Application to Engineering and Computer Science.* Prentice- Hall, India: George forstyle.

S.A.S. Sureni Wickramasooriya earned her B.Sc. Special degree in mathematics in 2014 and currently working as a Lecturer at the Department of Mathematics, Faculty of Engineering, University of Moratuwa**.**

Thisal M. Weerasekara earned his B.Sc. Special degree in mathematics in 2015 and currently working as an Instructor at the department of Mathematics, Faculty of Applied Sciences, University of Sri Jayewardenepura**.**

G.H. Jayantha Lanel earned his Ph.D. from University of Oakland and currently working as a Senior Lecturer at the department of Mathematics, Faculty of Applied Sciences, University of Sri Jayewardenepura**.**

T.P. de Silva earned her M.Sc. from Monash University and currently working as a Senior Lecturer at the department of Mathematics, Faculty of Applied Sciences, University of Sri Jayewardenepura

N.C. Ganegoda earned his Ph.D. from University of Sri Jayewardenepura and currently working as a Senior Lecturer at the department of Mathematics, Faculty of Applied Sciences, University of Sri Jayewardenepura**.**